### 1.3.1 Approach to Ensure Infrastructure Security [L.34.1.3.1]

***Agencies are supported by continuous oversight and processes to provide a secure infrastructure designed to protect critical data on both physical and logical levels.***

Network security is a cornerstone of AT&T's network philosophy. By following the security policy mandate of AT&T's Chief Executive Officer (CEO) as well as applicable regulations and legislation, AT&T protects its own information and resources and customers from unauthorized access, disclosure, corruption, or disruption of service. This security policy is applicable to AT&T network elements, systems, applications, and workstations owned or managed. Execution of this policy is led by the AT&T security organizations at the corporate and worldwide operational units. Security has ultimate responsibility for all aspects of network security. Specifically, security's role is to perform the following tasks:

- Own and manage security standards and guidelines
- Protect managed assets
- Supply security guidance and strategic direction to the business, worldwide security, and operations groups
- Provide consistent compliance globally to the network security program
- Implement and practice security standards
- Provide accountability of senior executives for security compliance in their business or region
- Coordinate a security review program to measure the degree of security compliance
- Maintain awareness of security industry changes and trends
- Develop and manage the corporation's global security education program

- Deliver security alerts and advisories to the corporate and worldwide service organizations
- Provide security specialist support to the operations and security teams
- Monitor and facilitate compliance with legal and regulatory security requirements.

[redacted] In addition, security standards, operating procedures, tools, and other protective measures are reviewed regularly to verify that high standards of security are observed throughout the company.

As the Information Technology (IT) environment and IT security concerns change, AT&T is helping to mold the next iteration of standards. AT&T is an active member/leader/founder of several standards committees and consortia at the state, national, and international levels. AT&T approach security architecture is summarized in **Table 1.3.1-1**.

| SECTION | SECTION DESCRIPTION |
|---|---|
| Section 1.3.1.a | Presents AT&T Protection Mechanism: Separation; Automation; Monitoring; Control; Testing; Response; Innovation |
| Section 1.3.1.b | Presents AT&T's measures to prevent cyber attacks<br>• Follow Defined Network Management Techniques<br>  • Configuration Management<br>  • Enterprise Network Management<br>  • Automated Provisioning systems<br>• Comprehensive Incident Detection and Response<br>  • Various system tools to detect and mitigate security risks |
| Section 1.3.1.c | Presents AT&T's approach to upholding best practices<br>• AT&T is a leader in setting industry best practices<br>• Security is designed into architecture of our network |
| Section 1.3.1.d | Presents AT&T's perspective on future security enhancements that will become available during Networx contract |

| SECTION | SECTION DESCRIPTION |
|---|---|
| Section 1.3.1.e | Presents AT&T's abilities to perform Certification and Accreditation (C&A) activities<br>• Trained, experienced, and cleared personnel<br>• AT&T C&A methodologies based on FIPS Publication 800-37<br>• Comprehensive C&A documentation and tools |

**Table 1.3.1-1: Response Summary for Section 1.3.1.** *Agencies acquire a comprehensive, proven security solution that provides protection for supported networks.*

Securing the Government's network is a high priority to AT&T. AT&T has supported the Government in the past with securing their applications and will continue to provide security protection in the future.

## 1.3.1.a Security Mechanisms and Controls [L.34.1.3.1.a]

(a) Describe the mechanisms and controls that the offeror uses in its network(s) to ensure protection of the offeror's infrastructure and provide security for the services offered to its customers.

*To keep Agencies' traffic secure, service providers must secure their network infrastructure.*

Agencies benefit from the mechanisms and controls AT&T uses in protecting our own network and providing worldwide network services to businesses in over 50 countries The AT&T global network consists of multiple components which are [redacted] The IP network supports global Internet access services, IP MPLS-enabled virtual private network (VPN) services, and various services implemented in networked server complexes (e.g., voice over Internet protocol [VoIP], email/ domain name service [DNS], application hosting, network-based managed firewalls, and management of customer premises equipment [CPE]).

[redacted]

[redacted]

At the network edge, AT&T has a rigorous set of security methods, processes, techniques, and practices [redacted] This is a necessary protection of the integrity and privacy of a VPN. A carrier must, however, also protect the service infrastructure against compromise or overload that might subvert the VPN.

[redacted]

[redacted]

| | |
|---|---|
| [redacted] | |
| [redacted] | |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | |
| [redacted] | |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | |
| [redacted] | |

| [redacted] | |
|---|---|
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | |
| [redacted] | |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | |
| [redacted] | |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | |
| [redacted] | |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | |
| [redacted] | |
| [redacted] | [redacted] |

[redacted]

The services provided to the Agencies are shielded from security threats because AT&T follows best practices and incorporates extensive security methods to protect our network infrastructure. AT&T maintains an ongoing security practice with the U.S. Government and welcomes the opportunity to expand that practice with the Agencies.

### 1.3.1.b Measures to Protect Against Cyber Attacks [L.34.1.3.1.b]

(b) Describe the measures to provide protection to the offeror’s infrastructure against cyber attacks (e.g., Bearer Independent Call Control (BICC), Denial of Service (DoS), Domain Name Server (DNS), H.323, Media Gateway Control Protocol (MGCP), and SS7 attacks, Spoofing, routing table corruption).

As a global communications carrier, AT&T has a twofold security environment to manage: [redacted] AT&T develops security innovations and deploys them on its corporate Intranet first. Next, it leverages those innovations and brings them to its various service networks. Finally, it uses them to assist enterprise customers with their own security management challenges.

### 1.3.1.b.1 Network Management Security Protection Methods

[redacted] how we protect our network and the services that we offer to Agencies in the categories of enterprise network management, IP network configuration management, and automated network provisioning and configuration tools. Agencies will benefit from the security that AT&T applies to its network and services from AT&T's ability to thwart attempted intrusions to the network and AT&T's services. In those cases where engineering and implementation are required for security services, AT&T deploys protections and disciplines on Agencies' own internal networks.

*Stopping cyber attacks in the network will mitigate cyber attacks on Agencies' applications.*

| | |
|---|---|
| [redacted] | |
| [redacted] | |
| [redacted] | |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | |
| [redacted] | [redacted] |
| [redacted] | |
| [redacted] | |
| [redacted] | [redacted] |

[redacted]

| | |
|---|---|
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |

[redacted]

### 1.3.1.b.1.1 Enterprise Network Management

[redacted]

### 1.3.1.b.1.2 IP Network Configuration Management

[redacted]

[redacted]

### 1.3.1.b.1.3 [redacted]

[redacted]

### 1.3.1.b.2 Incident Detection Security Protection Mechanisms

AT&T has invested significantly in the development of tools and resources to detect attacks emanating from the global Internet. These tools and resources allow AT&T to predict many Internet events before they became full-blown incidents. This capability protects AT&T's infrastructure and the services that will be provided to Agencies. [redacted] summarizes those Internet-specific security infrastructures.

*Automated tools and well-defined processes allow AT&T to quickly detect and defeat cyber attacks.*

[redacted]

| | |
|---|---|
| [redacted] | |
| [redacted] | |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |

[redacted]

[redacted]

[redacted]

### 1.3.1.b.3 Incident Response and Remediation Security Protection Mechanisms

*The best defense against cyber attacks is early identification and a speedy response.*

AT&T has developed security-related resources, both to respond to security incidents affecting AT&T as both an enterprise and a service provider. Several organizations within AT&T respond to suspected security incidents and provide remediation. Their specific areas of expertise and responsibility are detailed below.

[redacted]

[redacted]

[redacted]

### 1.3.1.b.4 Cyber Attack Prevention

[redacted]

[redacted]

| | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
|---|---|---|---|---|---|---|
| | [redacted] | | | | | |
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | | [redacted] | | |
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] | | [redacted] | [redacted] |
| [redacted] | [redacted] | | [redacted] | | | |
| [redacted] | [redacted] | [redacted] | [redacted] | | [redacted] | [redacted] |
| [redacted] | | [redacted] | | [redacted] | [redacted] | [redacted] |
| [redacted] | | [redacted] | | [redacted] | [redacted] | [redacted] |
| | [redacted] | | | | | |
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | | [redacted] | | |
| | [redacted] | | | | | |
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |

[redacted]

[redacted]

Multiple systems and procedures are used to protect the network from cyber attacks. [redacted]

[redacted]

[redacted]

[redacted]

### 1.3.1.b.5 Customer Security Protection Mechanisms

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Agencies benefit from the security measures (described above) to provide protection against cyber attacks to AT&T's infrastructure. Those benefits are extended to AT&T's managed security services, which will help guard Agencies' networks against hostile attacks. AT&T's approach to security considers the sum total of protections offered in the separate security services and how those will best be used to provide a greater degree of security protection more cost effectively.

[redacted]

[redacted]

## 1.3.1.c Application of Security and Reliability Best Practices [L.34.1.3.1.c]

(c) Describe how the network architecture is consistent with best practices for security and reliability.

AT&T's security expertise exemplifies the due diligence and discipline that a service provider provides to successfully protect its network and computing infrastructures, as well as those of Agencies. AT&T uses industry standards and our own best practices when designing methods and procedures to provide safe, reliable services. [redacted]

*By following Security Best Practices, AT&T continues to thwart future security attacks.*

[redacted]

[redacted]

| | |
|---|---|
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |

[redacted]

AT&T follows a well-defined process for designing security into every service or feature, from security architecture to deployment. [redacted]

[redacted]

| | |
|---|---|
| [redacted] | [redacted] |
| [redacted] | [redacted] |

[redacted]

| | |
|---|---|
| | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |

[redacted]

## 1.3.1.d Approach to Incorporating Security Enhancements [L.34.1.3.1.d]

(d) Describe the approach for incorporating into the offeror's network, infrastructure security enhancements that the offeror believes are likely to become commercially available in the timeframe covered by this acquisition. Include a discussion of potential problems and solutions.

Security continues to be critical in this new era to counter the growing threat of attacks from ever-more sophisticated cyber terrorists and criminals. With continued commitment to security discipline, AT&T develops new practices and technologies that enhance security. In addition, many vendors develop new technologies to enhance security, on all possible fronts. [redacted]

[redacted]

| | |
|---|---|
| [redacted] | [redacted] |

[redacted]

| | |
|---|---|
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |

[redacted]

### 1.3.1.d.1 Services over IP Security

Over the term of the contract, the Agency can anticipate that AT&T will continue to introduce innovative security technologies into the network. [redacted]

[redacted]

### 1.3.1.d.2 Storage Area Networks

Storage area network (SAN) is a popular tool offering a growing availability of bandwidth and a growing dependency on the data available on our systems' remote backup services. This is likely to become popular, especially with distributed mobile workforces. [redacted]

### 1.3.1.d.3 Mobile and Remote Users

Looking into the future, the growing availability of high-speed mobile connections allows users to always be in connection with information. Small devices can be effortlessly networked with large data stores back at the home office. With increasing reliance on data stored remotely, the availability and integrity of the data are essential. [redacted]

### 1.3.1.d.4 Identity Systems

As the network and real world continue to overlap and enhance each other, identity will become a significant issue. [redacted]

[redacted]

AT&T is committed to developing new network-based security services, such as an identity system network. AT&T has developed numerous security innovations and management techniques supporting security and has leveraged these security innovations to create services to support enterprises. AT&T's commitment to security will continue well into the 21st century, as security will become increasingly challenging. Based on these technology trends, AT&T predicts the emergence of a global, virtual society. In this society, mobility will be the norm as businesses and consumers demand a multitude of digital services that can be accessed from anywhere, at anytime, and by anyone (or by anything, e.g., appliances) over IP networks.

### 1.3.1.e Certification and Accreditation (C&A) Experience [L.34.1.3.1.e]

(e) Describe the offeror’s experience in supporting the Government in developing the documentation required in the Certification and Accreditation (C&A) process. (see National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS) PUB 800-37 — Guide for the Security Certification and Accreditation of Federal Information Systems).

[redacted]

[redacted]

| | |
|---|---|
| [redacted] | [redacted] |

[redacted]

| | |
|---|---|
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |

[redacted]

### 1.3.1.e.1 AT&T Information Assurance (IA) Team

[redacted]

[redacted]

[redacted]

### 1.3.1.e.2 C&A Guidelines

[redacted]

### 1.3.1.e.3 C&A Documents and Tools

[redacted]

[redacted]

| | | |
|---|---|---|
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]